Painting Your Home Blue

David Cypher

Advanced Network Technologies Division (ANTD) / ITL / NIST
(301) 975-4855, Fax: (301) 590 0932
david.cypher@nist.gov

When looking to network devices in the home, one should look at the Bluetooth™ wireless technology. The Bluetooth wireless technology was designed to be a cable replacement, but is being pushed to be much more. The Bluetooth wireless technology consists of two base documents and numerous others, including at least one on testing. The primary is the core specification. Within this document of over 1,000 pages are the protocols defined for all layers from the physical interface (i.e. radio interface) to the application level. The secondary is the profile specification. This document with almost 500 pages defines a number of profiles to be used with the core protocols to accomplish a particular application.

The core specification can be broken down into three major parts. The first is the part that contains the lower layer protocols. These lower layer protocols provide the wireless interface, the data link functions, and networking. The higher layer protocols provide the application specific items. The Host Controller Interface (HCI) that when present provides a defined interface for linking these other two major parts. This paper concentrates on the lower layer protocols and the HCI.

The lower layers are subdivided into the Radio, Baseband, Link Manager Protocol (LMP), and the Logical Link Control and Adaptation Protocol (L2CAP). By examining these lower layer protocol one can learn whether this wireless technology provides the functions necessary for a particular networking application.

The higher layers consist of the unique Service Discovery Protocol (SDP), RFCOMM, and Telephony Control Protocol. Two parts are concerned with providing interoperability with other protocols. These are the IrDA interoperability (OBEX), and Interoperability Requirements for Bluetooth as a Wireless Application Protocol (WAP).

The Host Controller Interface defines a physical interface structure between the upper and lower layers and does it using three different transport layers. The three supported transport layers (or replaced cable types) USB, RS232, and UART.

Following a more detailed description of these areas, this paper will describe the effort to create a formal description of the lower layer protocols as part of the standardization by IEEE 802.15.

This paper concludes with a description of the application profiles. This will open the window on where the Bluetooth wireless technology should be applied.

Painting Your Home Blue
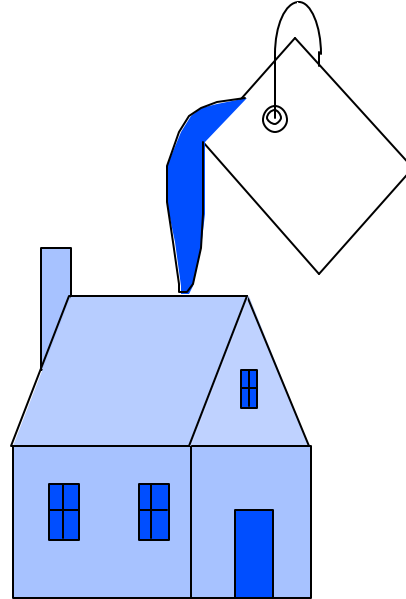
David Cypher

Information Technology Laboratory

Bluetooth™ Wireless Networking Technology

- Designed to be a cable replacement
- Short range ~10 meters
- Data rates < 1 Mbit/s
- Voice = 64 kbit/s
- Complete and interoperable systems
- 2.4 GHz ISM band (frequency hopping)
- Low cost

Bluetooth™ Wireless Networking Technology (Specifications)

- Core Specification
  - Revised many times (1.0, 1.0A, 1.0B, 1.1, 1.2 TBR)

- Assigned Numbers (1.1)

- Profile Specification (1.1)

- Test Specification (?)

Core Specification
(draft IEEE 802.15.1)

- Radio

- Baseband

- Link Manager Protocol (LMP)

- Logical Link Control and Adaptation Protocol (L2CAP)

- Host Controller Interface (HCI)
  - USB, RS232, UART

Core Specification

- Service Discovery Protocol (SDP)
- RFCOMM with TS 07.10
- IrDA Interoperability
- Telephony Control Protocol
- Interoperability Requirements for Bluetooth as a Wireless Application Protocol (WAP) Bearer
- Testing: mode, compliance, and control

Radio

- 2.4 GHz ISM (2402 - 2480 MHz)
- 1600 Hops/second
- Power classes
  - 1   100mW
  - 2   2.5mW
  - 3   1 mW
- Modulation: Gaussian Frequency Shift Keying

Baseband

- Master/Slave
- Time Division Multiplexing
- 625 µseconds TX/RX slot
- 1250 µseconds TX/RX period
- Channels (Asynchronous Connection-Less (ACL) and Synchronous-Oriented (SCO))
- Packets (Access Code, Header, Payload)

Baseband

- Inquiry
- Page
- Connection
  - Active
  - Hold
  - Sniff
  - Park

Link Manager Protocol (LMP)

- Master/Slave
- Request / Response
  - Authentication
    - Pairing
    - Changing keys
      - link
      - temporary
      - semi-permanent
  - Encryption
  - Switch Master/Slave
  - Information
    - (LMP Version, Supported Features, Name Request)
  - Clock Offset
  - Slot Offset
  - Timing Accuracy
  - Paging Scheme
  - State changes
    - (Hold, Sniff, & Park)

Link Manager Protocol (LMP)

- QOS
- Dynamic change between DMx and DHx
- Multi-slot packets
- Link Supervision
- SCO links
- Power control
- Detach

L2CAP

- Protocol Multiplexing
  - Channel Identifiers
    - Signalling
    - Connectionless
    - Dynamically Allocated
  - Protocol/Service Multiplexer (PSM)
- Quality of Service
  - conveying of

- Segmentation & Reassembly
  - with the help of
    - Baseband
    - HCI
- Group Management

Host Controller Interface (HCI)

- Functional
  - Commands
  - Events
  - Data
- USB
- RS232
- UART

- Commands
  - Link Control
  - Link Policy
  - Host Controller & Baseband
  - Informational
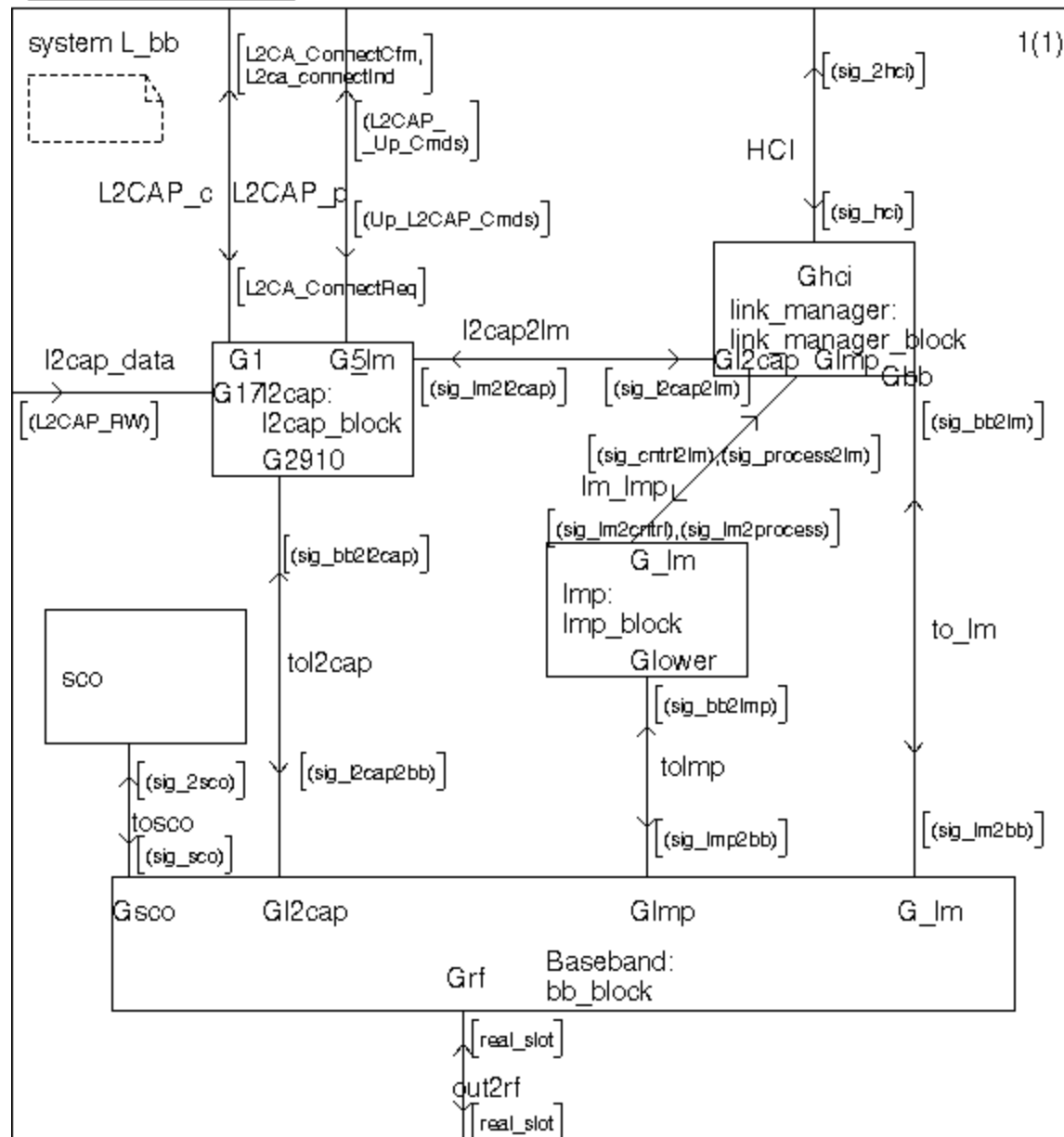 - Status
  - Testing
- Events
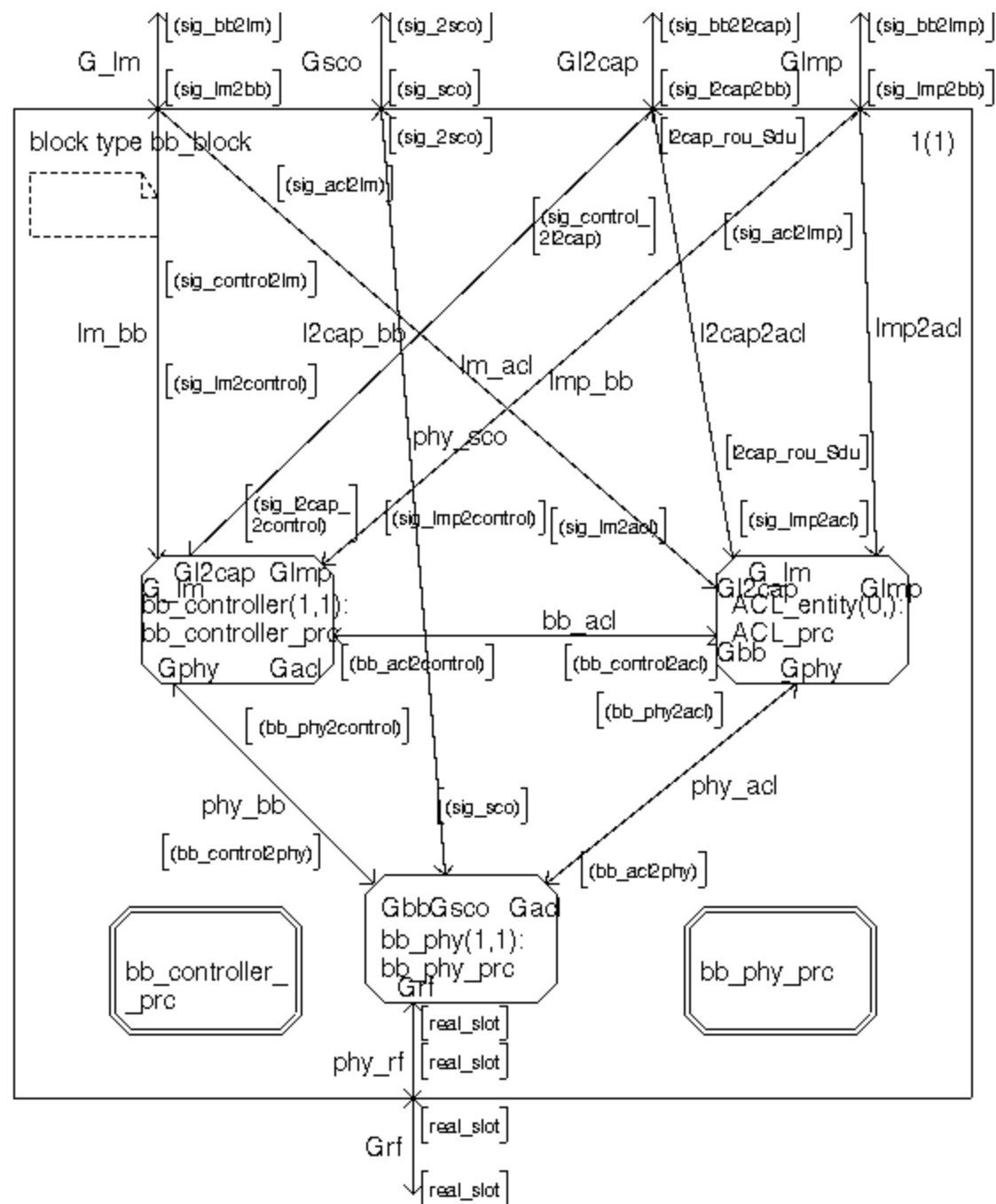- Data

Why a Formal Description?

- Text was
  - unclear,
  - ambiguous,
  - contradicting,
  - incomplete, &
  - open for
    - implementation &
    - interpretation

- Lack of
  - Service Access Points (SAP)
  - Single System View
  - Signal lists & interactions
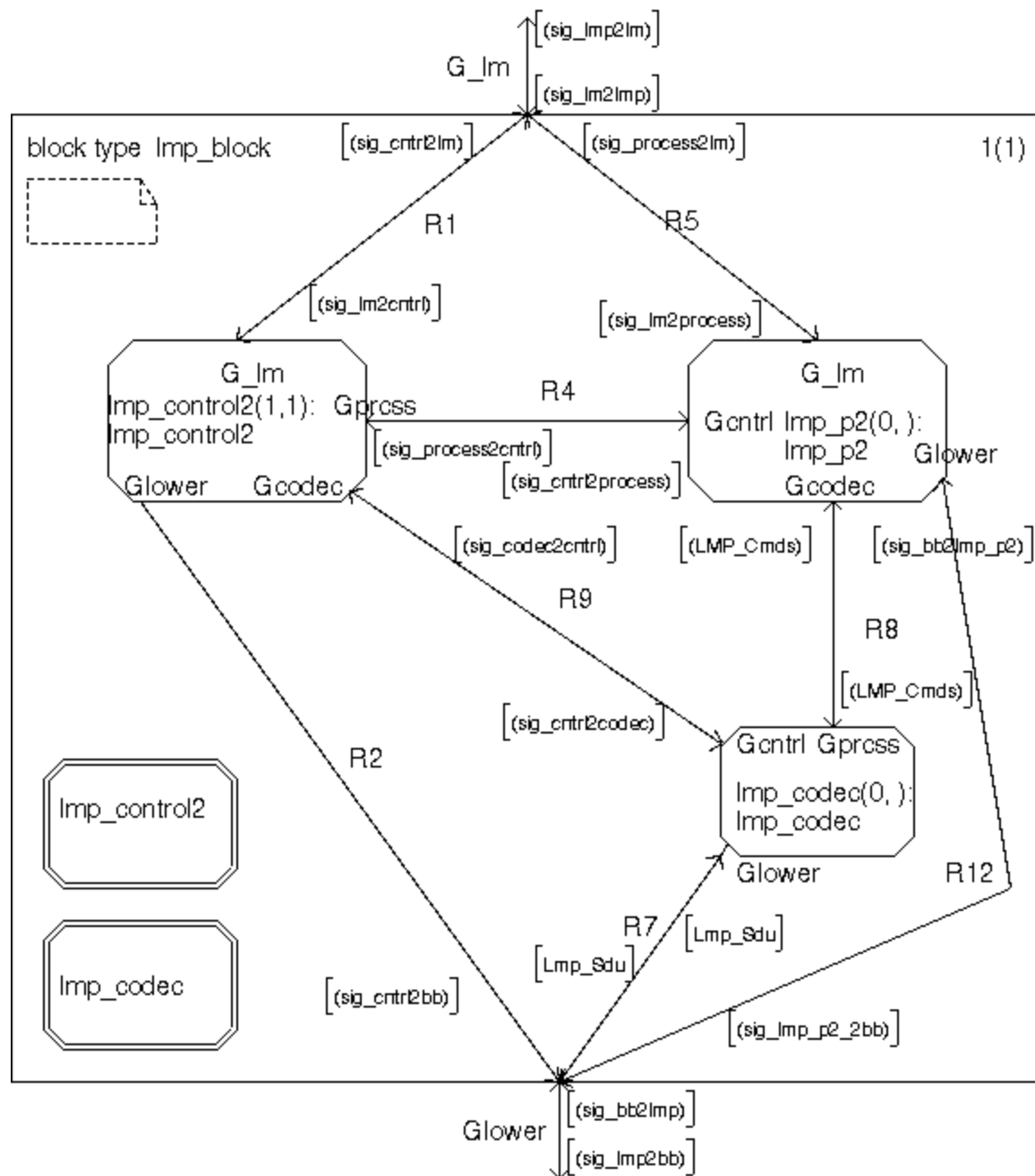
- Verify behavior
- Validate the protocol

block type link_manager_block

Ghci

[(sig_2hci), HCI_acl_data, HCI_sco_data]

[(sig_hci), HCI_acl_data, HCI_sco_data]

[(sig_2hci)]

1(1)

[HCI_sco_data]

[HCI_acl_data]

to_sco

to_acl

to_hci

[HCI_sco_data]

[HCI_acl_data]

Ghci
lm_sco(0,):
lm_sco
Gcontrol

Ghci
lm_acl(0,):
lm_acl
Gcontrol

[lm_terminate]

[lm_terminate]

R_sco

[(sig_hci)]

R_acl

Gsco   Ghci   Gacl

[(sig_lm2l2cap)]

link_manager_prc(1,1):
link_manager_prc

[(sig_lm2bb)]

Gl2cap   R_l2cap   Gl2cap   Gbb   R_bb   Gbb

[(sig_l2cap2lm)]

[(sig_lm2l2cap)]

[(sig_bb2lm)]

[(sig_bb2lm)]

[(sig_l2cap2lm)]

Glmp

[(sig_lm2bb)]

[(sig_lmp2lm)]

link_manager_prc

R_lmp_c

[(sig_lm2lmp)]

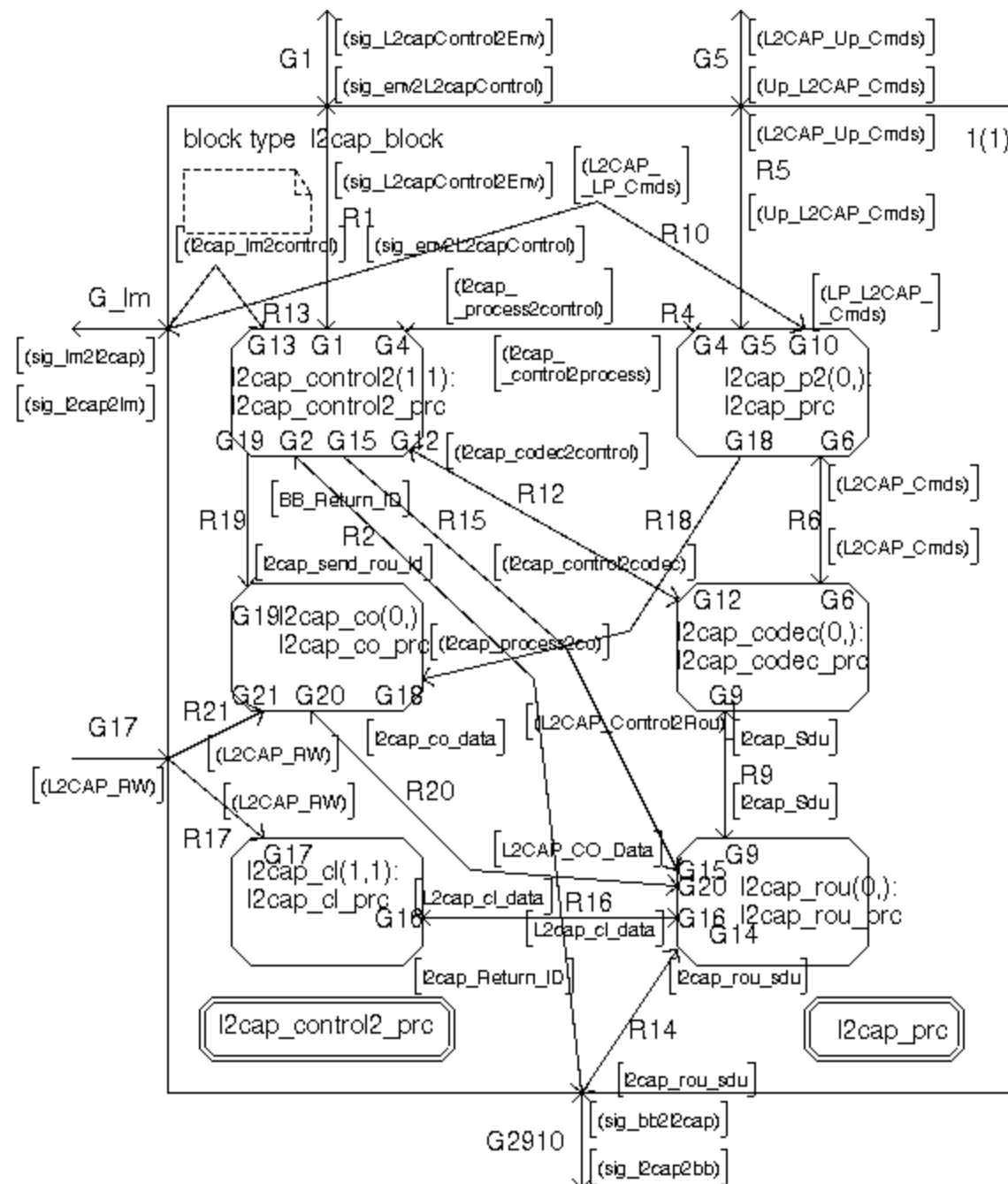Glmp

[(sig_lmp2lm)]
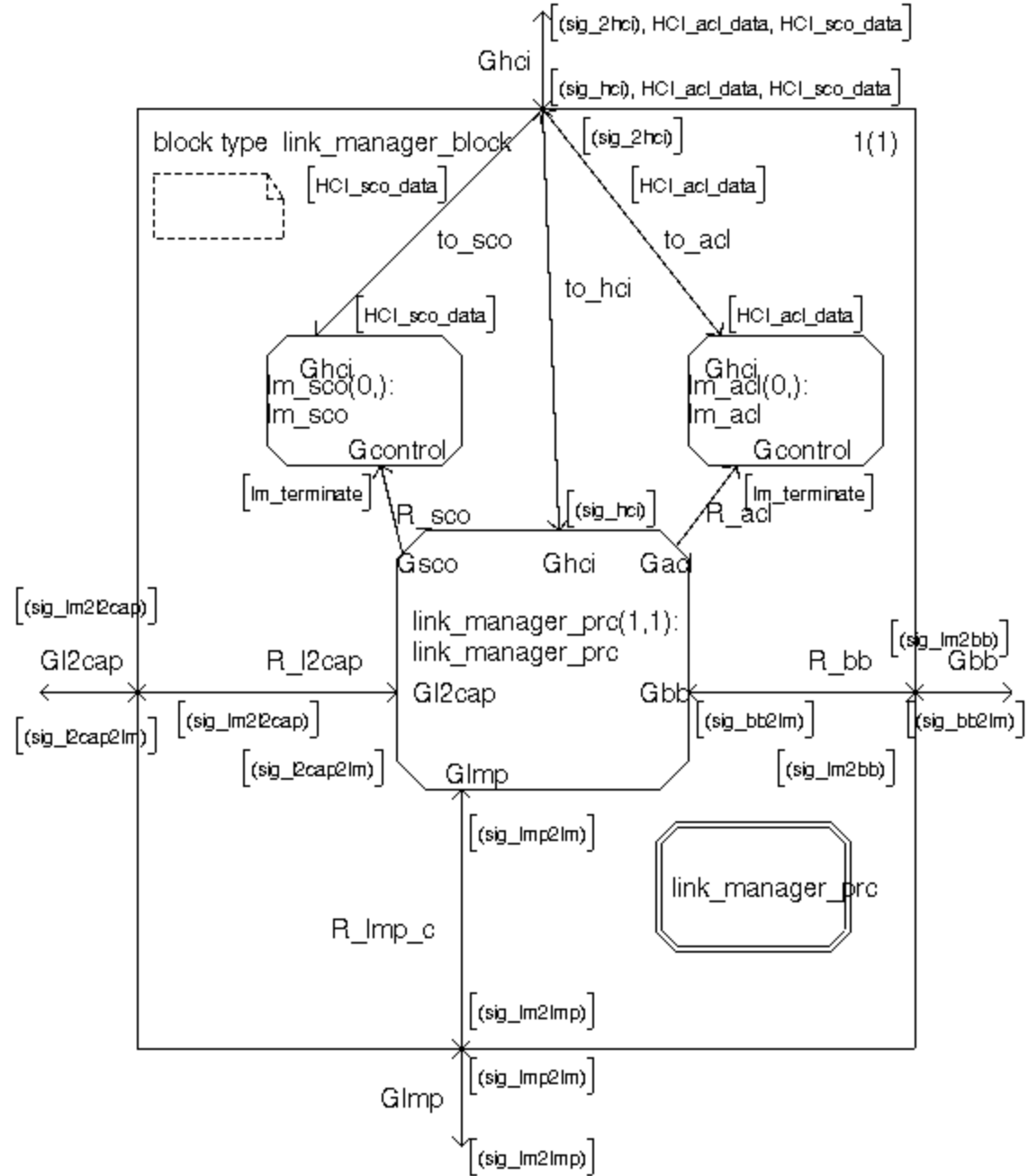
[(sig_lm2lmp)]

Profiles

- Generic Access
  - Service Discovery Application
  - Cordless Telephony
  - Intercom
  - Serial Port
    - Headset
    - Dial-up Networking
    - Fax
    - LAN Access
  - Generic Object Exchange
    - Object Push
    - File Transfer
    - Synchronization